Naval Surface Warfare Center, Crane Division
Technology Areas Attachment
for Strategic & Spectrum Missions Advanced Resilient Trusted Systems (S²MARTS)
Other Transaction Authority (OTA)

Technology Areas

The technology areas of current, specific interest to the Strategic & Spectrum Missions Advanced Resilient Trusted Systems (S²MARTS) Consortium-Model Other Transaction Authority (OTA) are described in this document. The technologies listed are only examples of technologies and are not limiting in scope. The intent is to ensure as new technological developments occur, Strategic and Spectrum Missions projects will be able to achieve rapid access to SOTA advancements. Therefore, the Technology Areas Attachment Document will evolve and change over the term of the agreement. Government mission need statements; request for white papers; request for prototype projects and objectives; and potential follow-on production contingent on successful prototype completion; may be issued to the S²MARTS Consortium Manager (CM) and/or Consortium Members based on the following areas:

1. Verification and Validation - Development, demonstration, and exploitation of technologies, algorithms, and methods that expands the ability and improves microelectronics test and verification methodologies in support of verifying the trust and assurance of parts.

2. Machine Learning - Development, demonstration, and exploitation of technologies, algorithms, and methods that expand the ability of a computer to learn from data, other computers, or sensors, without human intervention. Machine Learning computers can improve themselves from data, knowledge, experience and interaction with other computers. A computer with machine learning capabilities will use elements of statistics, knowledge science, computer science/systems, natural language processing, large database construction and management, and planning and control to improve its ability to suggest or predict outcomes of situations.

3. Multispectral Sensing – Development, demonstration, and exploitation of technologies, algorithms, and methods that expands the ability and improves sensors operating in the electromagnetic spectrum.

4. Design Assurance - Development, demonstration, and exploitation of technologies, algorithms, and methods that expands the ability for assured and immediate access to domestic production of advanced microelectronics and disruptive research and development investments to surpass the impending limitations of Moore's Law on silicon microelectronics. Innovative designs, models and prototypes are desired to enhance Electronic design automation (EDA) Tools; reverse engineering tools and demonstrations; intellectual property (IP) capture and library development; develop & demonstrate IP protection techniques, processes and prototypes; system on chip (SOC) development, prototyping, demonstration and capability insertion; obfuscation development and prototyping; hardware Trojan evaluation, test development & prototype demonstration; and image process development, prototype demonstration & automation.

5. Field Programmable Gate Arrays (FPGAs) are utilized in nearly all DoD Weapon systems and a significant element of the Trusted and Assured Microelectronics (T&AM) strategy is to ensure the ability to ensure trusted FPGA devices. Achieving the objective will require novel and unique methods including but not limited to: design, manufacturing, imagining, tagging, control and assessment approached for protecting the DoD's supply chain and intellectual property of the next generation of FPGA technology for defense end-use, advancing the U.S. and allied nations' technical superiority. Prototype development and demonstration in the areas of State-Of-The-Art (SOTA) trusted FPGAs; FPGA Analysis Tools; FPGA Built-In-Self-Tests (BIST); and FPGA Supply Chain Protection Techniques.

6. Enhanced Fabrication - Defense programs use commercial off-the-shelf (COTS) microelectronic assemblies within their system designs. These assemblies do not incorporate trust (synonymous with hardware assurance) architectures to ensure detection of and protection from hardware Trojans. Develop and demonstrate design, fabrication, and packaging techniques to ensure trust in microelectronic hardware assemblies that utilize state-of-the-art (SOTA) technologies to include 2.5D and 3D fabrication. Fabricating prototype hardware that incorporates the demonstrated trust techniques to validate and verify innovative techniques.

7. Radiation Hardened Microelectronics – Development, demonstration, and exploitation of technologies, algorithms, and methods that expand the ability for innovative design, manufacturing, and assessment approaches for trusted, strategic radiation-hardened (RAD-HARD) electronics in advanced technology nodes for next-generation strategic systems. This may include, but is not limited to RAD-HARD by Design (RHBD) for development of innovative techniques, characterization of radiation performance of alternate sources (foundry's) including advanced technology nodes, modeling to predict radiation response and investment to lead development of the next generation of radiation hardened microelectronics technology for defense end-use, advancing the U.S. and allied nations' technical superiority. RAD-HARD by process Research and Development (R&D), prototyping, demonstration and Strategic Radiation Hardened Electronics Council (SRHEC) process development and standards are also areas for innovation.

8. Outreach and Standards - Develop standards and practices to foster commercial development of secure, trusted and assured parts. Document and promulgate security-enhancing design practices across government, industry, and academia in the areas of standard program outreach material; standard training material; Government and industry standards and best practices; and self-service libraries of standards and best practices.

9. Magnetic Random Access Memory (MRAM) - Development, demonstration, and exploitation of technologies, algorithms, and methods that expand the ability of MRAM technology. In order to fully evaluate and validate trust (synonymous with hardware assurance) of the MRAM devices, the Government requires access to test modes not

typically made available by manufacturers. Provide access to these test modes by reaching agreement with the manufacturers for access to the test mode IP, and provide engineering technical support for Government test engineers conducting verification and validation tests.

10. Materials and Processes – Develop prototype technologies that will result in alternative materials or surrogate (next generation) materials for those no longer available from a source that meets the trust requirements of U.S. Military programs. Materials, electronics packaging technologies, or processes that improve the performance, reliability, or availability of high-power RF amplifiers and Electronic Warfare systems. Efforts include prototype hardware or materials demonstrating the developed technology. Areas of interest include: defense manufacturing parts, radomes, metamaterials, tools and capabilities applicable to microelectronics, printed circuit boards, wave guides, amplifiers, RF apertures, and interconnects.

11. Manufacturing Technology - Develop advanced prototype microelectronic components for use in multispectral sensors, high-power RF amplifiers, navigation, precision timing, and communications systems. This includes the development of algorithms, measurement techniques, hardware, and techniques to validate the reliability and maintainability of DoD required systems and components. Interest in counterfeit electronics component detection technology and mitigation techniques.

12. Modeling and Simulation - Develop and demonstrate virtual prototype models to support the component, system, engagement, and mission level. Includes prototypes that allow the interconnection of hardware in the loop with computer models and/or the use of virtual and augmented reality. Applications may include defense weapon system supply chain risk management (SCRM), electronic warfare engagements, cyber vulnerability threat analysis, and innovative uses of technology to achieve military advantage

13. Radio Frequency (RF) and Optoelectronic (OE) Microelectronics – Support secure design of RF and OE IP in all domestic major foundries. RF & OE prototyping across DoD and National Nuclear Security Administration (NNSA). Fabrication of novel RF & OE designs in state of the practice (SOTP) and SOTA foundries or critical DoD needs. Enhanced lithography and process capabilities of SOTP for RF & OE R&D for DoD and commercial use to gain a competitive advantage over adversaries.

14. New Microelectronics Development, Demonstration, and Capability Insertion - Public/private co-development of system-on-chip (SoC) that give 1000x performance improvement for DoD and commercial applications, through competition; hardware assurance, emulation and virtual verification and validation (V&V) to enable assured and secure IP; fabrication and packaging at SOTP government and merchant foundries; and design, packaging, testing, and integration of SoCs into a capability. This investment is intended to ensure that the most significant, new microelectronics devices, supporting

artificial intelligence (AI) applications, robust communications, and big data processing, sensor fusion, address United States Government (USG) and industry needs and allow for rapid insertion into acquisition systems with assurance and security.

15. Commercial-off-the-shelf (COTS) programmable integrated circuit (IC) co-development – Design, develop, prototype and demonstrate COTS devices at the leading edge with commercial partners matching to deliver assured FPGAs, graphics processing units (GPUs), machine learning, and data processing parts that meet current future DoD needs at commercial cost and timelines. Prototype software assurance and hardware assurance tools and security features and secure design environments for the development of these parts support proactive awareness and security.

16. Microelectronics Obsolescence and Replacement – Design, develop, prototype and demonstrate and support the rapid replacement of entire obsolete boards with a single SoC part, eliminating the legacy supply chain risks and deliver a future proof technology without having to upgrade software systems. Secure designs environments and V&V supercomputers will ensure full software and system integration and compatibility. Support critical process IP (IBM 9LP, 130SF) installation at one to two USG and/or merchant foundries for USG use. This IP is required to ensure the continued availability of these critical technologies by providing for second sources. It is needed to install IP purchased from Global Foundries (GF) in FY19 while GF subject matter expertise is available and current in the technologies.

17. Radiation Hardened by Process (RHBP)/Radiation Hardened by Design (RHBD) – Develop processes for SOTP access for 90nm, with path to 65nm technology node for strategic RHBP for Joint Federated Assurance Center (JFAC) and NNSA evaluation and qualification. Support secure design of RHBD IP in all major domestic foundries and fabrication of SOTA test articles for evaluation and qualification by JFAC and NNSA. Develop prototype proactive awareness and security.

18. Microelectronics and Electronic Warfare focused Workforce Development: - Develop access to training and skill development for university, DoD, and small businesses. This includes SOTA processes for test articles and training; promoting design challenges and hacks around hardware IP development/assurance.

19. Strategic Missions hardware related to nuclear deterrence, anti-tamper; cyber hardware security; ballistic missile launcher, fire control, navigation, guidance, and ballistic missile hardware; model based systems engineering; hypersonics models, simulation and prototypes; underwater launch models, simulations and prototypes and design enhancements.

20. Spectrum Warfare Technologies related to cognitive/adaptive, distributed/networked multispectral sensors, high power RF, spectral agility, low probability of intercept communications, RF and infrared countermeasures, and coherent RF transmission.

21. Spectrum Warfare Technologies related to advanced and custom optics, advanced threat assessment and exploitation efforts.